

### ***In the Claims***

The status of claims in the case is as follows:

1        1.    [Currently amended] A method for providing local  
2        gateway support for multiple overlapping remote networks  
3        using source-in VPN NAT, comprising the steps of:

4            loading a plurality of overlapping connections, each  
5            including an inbound packet having a conflicting source  
6            IP address;

7            for each said connection, binding said source IP  
8            address or VPN connection name in a bind table with an  
9            internally routable and system-wide unique source IP  
10          address from an internal address pool; and

11          VPN network address translating outbound packets, each  
12          said outbound packet having a destination IP address,  
13          to determine a virtual private network connection for  
14          receiving said outbound packet.

1        2.    [Currently amended] ~~The method of claim 1, further~~

~~comprising the steps of:~~ A method for providing local gateway support for multiple overlapping remote networks, comprising the steps of:

loading a plurality of overlapping connections, each including an inbound packet having a source IP address;

for each said connection, binding said source IP address in a bind table with an internally routable and system-wide unique source IP address from an internal address pool;

network address translating outbound packets, each said outbound packet having a destination IP address, to determine a virtual private network connection for receiving said outbound packet;

filtering said outbound packet to determine a first connection name;

determining from said bind table a second connection name;

responsive to said first and second connection names

20 comparing equal, processing said outbound packet into a  
21 VPN tunnel using a security association database  
22 determined by said first connection name; and

23 responsive to said first and second connection names  
24 comparing not equal, processing said outbound packet  
25 into a VPN tunnel using a security association database  
26 determined by said second connection name.

1 3. [Original] A local gateway system, comprising:

2 an address pool for storing a plurality of internally  
3 routable and system wide, nonconflicting network  
4 addresses;

5 an address bind table for binding a conflicting source  
6 address from an inbound packet from a remote network to  
7 a connection name and to a unique network address from  
8 said address pool;

9 a filter rules table responsive to an outbound packet  
10 for determining a first connection indicia;

11 said address bind table further responsive to said

12           outbound packet for determining a second connection  
13           indicia; and

14           said local gateway system being responsive to said  
15           first and second connection indicia comparing equal for  
16           processing said outbound packet to a communications  
17           tunnel using a first security association determined by  
18           said first connection indicia, and responsive to said  
19           first and second connection indicia comparing not equal  
20           for processing said outbound packet to a communications  
21           tunnel using a second security association determined  
22           by said second connection indicia.

1       4.   [Currently amended] A program storage device readable  
2       by a machine, tangibly embodying a program of instructions  
3       executable by a machine to perform method steps for  
4       providing local gateway support for multiple overlapping  
5       remote networks using source-in VPN NAT, said method steps  
6       comprising:

7           loading a plurality of overlapping connections, each  
8           including an inbound packet having a conflicting source  
9           IP address;

10           for each said connection, binding said source IP  
11           address in a bind table with an internally routable and  
12           system-wide unique source IP address from an internal  
13           address pool; and

14           VPN network address translating outbound packets, each  
15           said outbound packet having a destination IP address,  
16           to determine a virtual private network connection for  
17           receiving said outbound packet.

1       5.   [Currently amended] ~~The program storage device of~~  
2   ~~claim 4, said method steps further comprising: A program~~  
3   ~~storage device readable by a machine, tangibly embodying a~~  
4   ~~program of instructions executable by a machine to perform~~  
5   ~~method steps for providing local gateway support for~~  
6   ~~multiple overlapping remote networks, said method steps~~  
7   ~~comprising:~~

8           loading a plurality of overlapping connections, each  
9           including an inbound packet having a source IP address;  
  
10          for each said connection, binding said source IP  
11          address in a bind table with an internally routable and  
12          system-wide unique source IP address from an internal

13           address pool;

14           network address translating outbound packets, each said  
15           outbound packet having a destination IP address, to  
16           determine a virtual private network connection for  
17           receiving said outbound packet;

18           filtering said outbound packet to determine a first  
19           connection name;

20           determining from said bind table a second connection  
21           name;

22           responsive to said first and second connection names  
23           comparing equal, processing said outbound packet into a  
24           VPN tunnel using a security association database  
25           determined by said first connection name; and

26           responsive to said first and second connection names  
27           comparing not equal, processing said outbound packet  
28           into a VPN tunnel using a security association database  
29           determined by said second connection name.

1       6.   [Currently amended]   A computer program product or

2 computer program element for providing local gateway support  
3 for multiple overlapping remote networks using source-in VPN  
4 NAT, according to method steps comprising:

5 loading a plurality of overlapping connections, each  
6 including an inbound packet having a conflicting source  
7 IP address;

8 for each said connection, binding said source IP  
9 address in a bind table with an internally routable and  
10 system-wide unique source IP address from an internal  
11 address pool; and

12 VPN network address translating outbound packets, each  
13 said outbound packet having a destination IP address,  
14 to determine a virtual private network connection for  
15 receiving said outbound packet.

1 7. [Original] A local gateway system for processing  
2 inbound and outbound packets with respect to a local network  
3 and a plurality of remote nodes having potentially  
4 overlapping addresses, comprising:

5 an address pool component;

6           an address bind table component;

7           a filter rules table component;

8           a security association component;

9           an entry in said address bind table component including  
10          a left hand side (LHS) address field, a right hand side  
11          (RHS) address field, and first connection name field;

12          an entry in said filter rules table component including  
13          source IP address (sip), destination IP address (dip),  
14          source port, destination port, second connection name,  
15          and action field;

16          said address pool component including a pool of sip  
17          addresses administratively reserved and uniquely  
18          routable within said local network;

19          a security association in said security association  
20          component including third connection name and security  
21          association data;

22          first logic responsive to an inbound packet for



23           dynamically binding in said address bind table  
24           component the inbound packet sip with a local sip  
25           selected from said address pool component and first  
26           connection indicia;  
  
27           second logic responsive to an outbound packet for  
28           accessing said filter rules table component to  
29           determine filter derived connection indicia;  
  
30           third logic responsive to said outbound packet for  
31           accessing said address bind table component to  
32           determine corresponding bind table derived connection  
33           indicia; and  
  
34           fourth logic responsive to said filter derived  
35           connection indicia and said bind table derived  
36           connection indicia comparing equal for accessing said  
37           security association component to select security  
38           association data corresponding to said filter derived  
39           connection data for processing said outbound packet,  
40           and responsive to said filter derived connection  
41           indicia and said bind table derived connection indicia  
42           comparing not equal for accessing said security  
43           association component to select security association

44 data corresponding to said bind table derived  
45 connection indicia for processing said outbound packet.

1 8. [Original] The local gateway system of claim 7,  
2 further comprising:

3 said action field selectively containing deny, permit,  
4 and IP Sec required indicia; and

5 said second logic being responsive to said outbound  
6 packet corresponding to a filter having an action field  
7 containing said IP Sec required indicia for initiating  
8 execution of said third logic.

1 9. [Currently amended] A method for operating a local  
2 gateway using source-in VPN NAT, comprising the steps of:

3 receiving an inbound packet having a conflicting  
4 source-in IP address on a network connection from a  
5 remote node; and

6 applying source-in network address translation to  
7 establish dynamic binding of the source IP address of  
8 said inbound packet with an internally routable and

9           system wide unique source-in IP address and a  
10           connection name.

1       10. [Currently amended] ~~The method of claim 9, further~~  
2       ~~comprising the steps of:~~ A method for operating a local  
3       gateway, comprising the steps of:

4           receiving an inbound packet on a network connection  
5           from a remote node;

6           applying source-in network address translation to  
7           establish dynamic binding of the source IP address of  
8           said inbound packet with an internally routable and  
9           system wide unique source-in IP address and a  
10          connection name;

11          receiving an outbound packet from an internal node;

12          filtering said outbound packet to determine a first  
13          connection;

14          selectively determining a second connection from a  
15          connection name bound to said unique source-in IP  
16          address corresponding to the destination-out IP address

17           of said outbound packet; and

18           selectively overriding said first connection by said  
19           second connection.

1       11. [Original] The method of claim 10, further comprising  
2       the step of:

3           tunneling said outbound packet to said remote node  
4           responsive to security association data selectively  
5           corresponding to said first connection or said second  
6           connection.

1       12. [Original] The method of claim 11, further comprising  
2       the step of:

3           overriding said first connection by said second  
4           connection responsive to said first connection and said  
5           second connection comparing not equal.

1       13. [Currently amended] A program storage device readable  
2       by a machine, tangibly embodying a program of instructions  
3       executable by a machine to perform method steps for  
4       providing local gateway support for multiple overlapping

remote networks using source-in VPN NAT, said method steps comprising:

receiving an inbound packet having a conflicting source-in IP address on a network connection from a remote node; and

applying VPN source-in network address translation to establish dynamic binding of the source IP address of said inbound packet with an internally routable and system wide unique source-in IP address and a connection name.

14. [Currently amended] ~~The program storage device of claim 13, said method steps further comprising:~~ A program storage device readable by a machine, tangibly embodying a program of instructions executable by a machine to perform method steps for providing local gateway support for multiple overlapping remote networks, said method steps comprising:

receiving an inbound packet on a network connection from a remote node;

10       applying source-in network address translation to  
11       establish dynamic binding of the source IP address of  
12       said inbound packet with an internally routable and  
13       system wide unique source-in IP address and a  
14       connection name;  
  
15       receiving an outbound packet from an internal node;  
  
16       filtering said outbound packet to determine a first  
17       connection;  
  
18       selectively determining a second connection from a  
19       connection name bound to said unique source-in IP  
20       address corresponding to the destination-out IP address  
21       of said outbound packet; and  
  
22       selectively overriding said first connection by said  
23       second connection.

1       15. [Original] The program storage device of claim 14,  
2       said method steps further comprising:

3       tunneling said outbound packet to said remote node  
4       responsive to security association data selectively

5 corresponding to said first connection or said second  
6 connection.

1 16. [Original] The program storage device of claim 15,  
2 said method steps further comprising:

3 overriding said first connection by said second  
4 connection responsive to said first connection and said  
5 second connection comparing not equal.

1 17. [Original] A communication method, comprising the  
2 steps of:

3 operating a remote gateway to initiate a connection  
4 with a local gateway;

5 sending from a remote node at said remote gateway an  
6 inbound packet addressed by a destination address to a  
7 local node at said local gateway and a remote node  
8 source address identifying said remote node;

9 operating said local gateway to decapsulate said  
10 inbound packet;

11        operating said local gateway to determine that said  
12        inbound packet requires source-in network address  
13        translation and that no existing address bind exists  
14        for said inbound packet;

15        operating said local gateway to choose a pool address  
16        and create a binding table entry binding said remote  
17        node source address to said pool address and a unique  
18        connection name;

19        replacing said remote node source address with said  
20        pool address and forwarding said inbound packet to said  
21        local node;

22        receiving at said local gateway an outbound packet  
23        having as its destination address said pool address;

24        filtering said outbound packet to identify  
25        corresponding connection indicia;

26        finding in said binding table an entry corresponding to  
27        said outbound packet, converting said destination  
28        address to said remote node source address, and  
29        returning said unique connection name;



30 responsive to said unique connection name, selecting  
31 security association data; and  
  
32 responsive to said security association data, tunneling  
33 said outbound packet to said remote node.

1 18. [Original] The method of claim 17, said remote node  
2 being one of a plurality of remote nodes having overlapping  
3 addresses.

1 19. [Original] The method of claim 18, further comprising  
2 the steps of:

3 comparing said corresponding connection indicia and  
4 said unique connection name; and

5 responsive to said corresponding connection indicia and  
6 said unique connection name comparing equal, selecting  
7 security association data corresponding to said  
8 corresponding connection indicia.

1 20. [Currently amended] A method for operating a local  
2 gateway for controlling communication between a local node  
3 and a remote node using source-in VPN NAT, comprising the

4 steps of:

5 receiving an inbound packet on a network connection  
6 from a remote node, said inbound packet characterized  
7 by a conflicting first source address identifying said  
8 remote node and a first destination address identifying  
9 said local node; and

10 applying VPN source-in network address translation to  
11 establish dynamic binding of said first source address  
12 with an internally routable and system wide unique  
13 second source address and a first connection name.

1 21. [Currently amended] ~~The method of claim 20, further~~  
2 ~~comprising the steps of:~~ A method for operating a local  
3 gateway for controlling communication between a local node  
4 and a remote node, comprising the steps of:

5 receiving an inbound packet on a network connection  
6 from a remote node, said inbound packet characterized  
7 by a first source address identifying said remote node  
8 and a first destination address identifying said local  
9 node;

10       applying source-in network address translation to  
11       establish dynamic binding of said first source address  
12       with an internally routable and system wide unique  
13       second source address and a first connection name; and  
  
14       establishing said dynamic binding by creating a binding  
15       entry in an address bind table with a bind entry left  
16       hand side set equal to said second source address  
17       selected from a local address pool, a bind entry right  
18       hand side set equal to said first source address, and  
19       said first connection name.

1       22. [Original] The method of claim 21, further comprising  
2       the steps of:

3       receiving from said local node an outgoing packet  
4       intended for said remote node and having identifying  
5       indicia including a second destination address;

6       filtering said outgoing packet to find a filter rule  
7       having a second connection name associated with said  
8       identifying indicia;

9       responsive to said second connection name, identifying

10           a filter derived security association;

11           responsive to said filter rule requiring source-in  
12           network address translation, searching said address  
13           bind table for a matching binding entry having a bind  
14           entry left hand side corresponding to said second  
15           destination address, and setting said second  
16           destination address equal to said bind entry right hand  
17           side;

18           responsive to said first connection name selected from  
19           said matching binding entry, identifying a binding  
20           table derived security association; and

21           selectively responsive to said filter derived security  
22           association or said binding table derived security  
23           association, processing said outbound packet into a  
24           tunnel for communication to said remote node.

1       23. [Original] The method of claim 22, further comprising  
2       the steps of:

3           responsive to said first connection name selected from  
4           said matching binding entry and said second connection

5           name comparing not equal, selecting said binding table  
6           derived security association for processing said  
7           outbound packet.

1       24. [Original] A program storage device readable by a  
2       machine, tangibly embodying a program of instructions  
3       executable by a machine to perform method steps for  
4       providing local gateway support for multiple overlapping  
5       remote networks, said method steps comprising:

6           operating a remote gateway to initiate a connection  
7           with a local gateway;

8           sending from a remote node at said remote gateway an  
9           inbound packet addressed by a destination address to  
10          said local node at said local gateway and a remote node  
11          source address identifying said remote node;

12          operating said local gateway to decapsulate said  
13          inbound packet;

14          operating said local gateway to determine that said  
15          inbound packet requires source-in network address  
16          translation and that no existing address bind exists

17           for said inbound packet;

18           operating said local gateway to choose a pool address  
19           and create a binding table entry binding said remote  
20           node source address to said pool address and a unique  
21           connection name;

22           replacing said remote node source address with said  
23           pool address and forwarding said inbound packet to said  
24           local node;

25           receiving at said local gateway an outbound packet  
26           having as its destination address said pool address;

27           filtering said outbound packet to identify  
28           corresponding connection indicia;

29           finding in said binding table an entry corresponding to  
30           said outbound packet, converting said destination  
31           address to said remote node source address, and  
32           returning said unique connection name;

33           responsive to said unique connection name, selecting  
34           security association data; and

35 responsive to said security association data, tunneling  
36 said outbound packet to said remote node.

1 25. [Currently amended] A program storage device readable  
2 by a machine, tangibly embodying a program of instructions  
3 executable by a machine to perform method steps for  
4 providing local gateway support for multiple overlapping  
5 remote networks using source-in VPN NAT, said method steps  
6 comprising:

7 receiving an inbound packet on a network connection  
8 from a remote node, said inbound packet characterized  
9 by a conflicting first source address identifying said  
10 remote node and a first destination address identifying  
11 said local node; and

12 applying VPN source-in network address translation to  
13 establish dynamic binding of said first source address  
14 with an internally routable and system wide unique  
15 second source address and a first connection name.

1 ~~26. [Currently amended] The program storage device of~~  
2 ~~claim 25, said method steps further comprising: A program~~  
3 ~~storage device readable by a machine, tangibly embodying a~~

4 program of instructions executable by a machine to perform  
5 method steps for providing local gateway support for  
6 multiple overlapping remote networks, said method steps  
7 comprising:

8 receiving an inbound packet on a network connection  
9 from a remote node, said inbound packet characterized  
10 by a first source address identifying said remote node  
11 and a first destination address identifying said local  
12 node;

13 applying source-in network address translation to  
14 establish dynamic binding of said first source address  
15 with an internally routable and system wide unique  
16 second source address and a first connection name; and

17 establishing said dynamic binding by creating a binding  
18 entry in an address bind table with a bind entry left  
19 hand side set equal to said second source address  
20 selected from a local address pool, a bind entry right  
21 hand side set equal to said first source address, and  
22 said first connection name.

1 27. [Original] The program storage device of claim 26,



2       said method steps further comprising:

3           receiving from said local node an outgoing packet  
4           intended for said remote node and having identifying  
5           indicia including a second destination address;

6           filtering said outgoing packet to find a filter rule  
7           having a second connection name associated with said  
8           identifying indicia;

9           responsive to said second connection name, identifying  
10          a filter derived security association;

11          responsive to said filter rule requiring source-in  
12          network address translation, searching said address  
13          bind table for a matching binding entry having a bind  
14          entry left hand side corresponding to said second  
15          destination address, and setting said second  
16          destination address equal to said bind entry right hand  
17          side;

18          responsive to said first connection name selected from  
19          said matching binding entry, identifying a binding  
20          table derived security association; and

21 selectively responsive to said filter derived security  
22 association or said binding table derived security  
23 association, processing said outbound packet into a  
24 tunnel for communication to said remote node.

1 28. [Original] The program storage device of claim 27,  
2 said method steps further comprising:

3 responsive to said first connection name selected from  
4 said matching binding entry and said second connection  
5 name comparing not equal, selecting said binding table  
6 derived security association for processing said  
7 outbound packet.